UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, Defendant.	Case No. CR19-159RSL ORDER DENYING MOTION TO DISMISS COUNTS 1, 9, & 10

This matter comes before the Court on defendant Paige Thompson's "Motion to Dismiss Counts 1, 9, and 10 of the Superseding Indictment." [1] (Dkt. # 122). Defendant faces an upcoming trial for charges of wire fraud, violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), access device fraud, and aggravated identity theft. Dkt. # 166. She contends that Count 1 of the indictment against her must be dismissed for failure to provide sufficient notice, and that Counts 9 and 10 must accordingly be dismissed as well, given that Count 1 forms the foundation for these later counts. Dkt. # 122 at 1-2. In the alternative, defendant asks that the Court order the government to provide a bill of particulars, outlining "the specific facts it intends to present at trial to prove Ms. Thompson committed wire fraud." *Id.* at 6.

[1] The government introduced a Second Superseding Indictment (Dkt. # 166) after briefing for this motion was submitted. Because the Second Superseding Indictment does not substantively modify Counts 1, 9 and 10, the Court reads the arguments in the present motion as applying equally to both versions of the Superseding Indictment and applies this ruling to the Second Superseding Indictment.

I. Sufficiency of Indictment

Under Federal Rule of Criminal Procedure 7(c)(1), the indictment "must be a plain, concise, and definite written statement of the essential facts constituting the offense charged." To pass constitutional muster, an indictment must "contain the elements of the charged crime in adequate detail to inform the defendant of the charge" and "enable [the defendant] to plead double jeopardy." *United States v. Buckley*, 689 F.2d 893, 896 (9th Cir. 1982); *see also Russell v. United States*, 369 U.S. 749, 763-64 (1962). "Because it is a drastic step, dismissing an indictment is a disfavored remedy." *United States v. Rogers*, 751 F.2d 1074, 1076-77 (9th Cir. 1985) (citing *United States v. Blue*, 384 U.S. 251, 255 (1966)).

Here, defendant moves to dismiss Counts 1, 9, and 10 of the indictment for "lack of specificity" and "failure to state an offense." Fed. R. Crim. P. 12(b)(3)(B)(iii), (v). At this motion to dismiss stage, "the issue in judging the sufficiency of the indictment is whether the indictment adequately alleges the elements of the offense and fairly informs the defendant of the charge, not whether the Government can prove its case." *Buckley*, 689 F.2d at 897. "The Government need not allege its theory of the case or supporting evidence, but only the 'essential facts necessary to apprise a defendant of the crime charged.'" *Id.* (quoting *United States v. Markee*, 425 F.2d 1043, 1047-48 (9th Cir. 1970)). An indictment need not explain all factual evidence to be proved at trial. *United States v. Blinder*, 10 F.3d 1468, 1476 (9th Cir. 1993).

In evaluating a motion to dismiss, the Court accepts the allegations in the indictment as true and is "bound by the four corners of the indictment." *United States v. Boren*, 278 F.3d 911, 914 (9th Cir. 2002). The indictment must be "construed according to common sense, and interpreted to include facts which are necessarily implied." *United States v. Berger*, 473 F.3d 1080, 1103 (9th Cir. 2007) (internal quotation marks and citation omitted). A motion brought pursuant to Federal Rule of Criminal Procedure 12(b)(3)(B) is "capable of determination before trial if it involves questions of law rather than fact" and therefore does not intrude upon "the province of the ultimate finder of fact." *United States v. Kelly*, 874 F.3d 1037, 1046-47 (9th Cir. 2017) (quotations omitted).

A. Basis for Wire Fraud Charge

The indictment alleges that defendant created proxy scanners that allowed her to identify Amazon Web Services servers with misconfigured web application firewalls that permitted outside commands to reach and be executed by the servers. Dkt # 166 at ¶ 12. Defendant then sent commands to the misconfigured servers to obtain security credentials for particular accounts or roles belonging to the victims. *Id.* at ¶¶ 11-13, 16-18. Defendant then used these "stolen credentials" to "copy data, from folders or buckets of data" in the victims' cloud storage space and set up cryptocurrency mining operations on the victims' rented servers. *Id.* at ¶¶ 14-15, 21. The indictment further alleges that defendant concealed her location and identity while executing these actions by using VPNs and TOR.[2] *Id.* at ¶¶ 17-18.

Defendant argues that the indictment fails to state a wire fraud offense because it neither alleges that she made any misrepresentation of material fact nor that she possessed the specific intent required under the statute. Dkt. # 122 at 6.

The elements of wire fraud are: (1) a scheme to defraud; (2) the use of a wire, radio, or television to further the scheme; and (3) a specific intent to defraud. *United States v. Lindsey*, 850 F.3d 1009, 1013 (9th Cir. 2017).[3] While "bare bones" indictments "employing the statutory language alone" are often permitted in the Ninth Circuit, *United States v. Woodruff*, 50 F.3d 673, 676 (9th Cir. 1995), where the offense contains "generic terms" the indictment must "descend to particulars," *Russell*, 369 U.S. at 763. "Indictments alleging a scheme to defraud must provide sufficient facts to fulfill the purposes of an indictment." *Buckley*, 689 F.2d at 897.

---

[2] VPNs (virtual private networks) and TOR (The Onion Router) are both technologies that facilitate online privacy and can be used to conceal a user's identity and/or location.

[3] Because the Supreme Court has clearly stated that the mail and wire fraud statutes should be interpreted in the same manner, *see Carpenter v. United States*, 484 U.S. 19, 25 n.6 (1987), this Order relies on precedent analyzing both statutes. Because the Supreme Court has interpreted the "scheme to defraud" element consistently across the bank, mail, and wire fraud statutes, *see Neder*, 527 U.S. at 20; *Miller*, 953 F.3d at 1102 n.7 ("Because the bank, mail, and wire fraud statutes all use highly similar language, we take the Supreme Court's reasoning . . . to apply to the wire fraud statute as well."), this Order relies on precedent analyzing any of the three statutes in assessing this element.

On a motion under Federal Rule of Criminal Procedure 12, the failure to allege facts that, if proven, would satisfy an essential element of the offense is a fatal defect requiring dismissal of the indictment. *See United States v. Omer*, 395 F.3d 1087, 1089 (9th Cir. 2005).

1. Element One: Misrepresentation

Defendant argues that the indictment fails in part because "Count 1 comes nowhere close to describing any misrepresentations or concealments of material fact by Ms. Thompson," and thus the first element of wire fraud is not sufficiently alleged. Dkt. # 122 at 6.

Proving a scheme to defraud requires showing a "misrepresentation or concealment of material fact." *Neder v. United States*, 527 U.S. 1, 21-25 (1999). There are "alternative routes" to reach this requirement – proof of a specific material false statement is not required. *United States v. Woods*, 335 F.3d 993, 999 (9th Cir. 2003). Instead, this element can be met by showing "proof of a scheme or artifice to defraud." *Id.*; *Omer*, 395 F.3d at 1089 (explaining that it is "the materiality of the scheme or artifice that must be alleged; the materiality of a specific statement need not be pleaded."). "[A]cts taken to conceal, create a false impression, mislead, or otherwise deceive in order to 'prevent the other party from acquiring material information'" may demonstrate a scheme to defraud. *United States v. Colton,* 231 F.3d 890, 898 (4th Cir. 2000) (quoting Restatement (Second) of Torts § 550 (Am. L. Inst. 1977)); *Woods*, 335 F.3d at 998. A falsehood "is material if it has a natural tendency to influence, or is capable of influencing, the decision of the decisionmaking body to which it was addressed." *Neder*, 527 U.S. at 16 (internal quotations and alterations omitted).

Defendant argues that the indictment fails to allege this first element of wire fraud. Specifically, defendant claims that (1) neither the use of TOR nor a VPN can be considered a misrepresentation, as neither are illegal or "nefarious," and (2) she did not make any materially false representations or omissions when accessing the misconfigured servers. *See* Dkt. # 158 at 2-3; Dkt. # 122 at 6.

The government counters that once defendant obtained security credentials for the accounts, she implicitly misrepresented herself as an authorized user when she used those stolen credentials to send commands to copy data. Dkt. # 166 at ¶ 16. The government further argues

that the "act of accessing a server with stolen credentials itself is a materially false pretense and representation." Dkt. # 131 at 6 (citing *United States v. Khalupsky*, 5 F.4th 279, 291 (2d Cir. 2021)). Additionally, the government argues that defendant exhibited a "scheme to defraud" through her pattern of conduct. *Id.* at 6-7. Namely, defendant used VPNs and TOR to "conceal her location and identity," then, while concealed, she used a scanner she had created to identify servers with misconfigured web application firewalls and obtained security credentials for those accounts. *Id.* Finally, using those stolen credentials, she copied data from the accounts, and used the computing power of the infiltrated servers to "mine" cryptocurrency. *Id.*

Regarding defendant's argument that the wire fraud count must be stricken because the underlying alleged acts were not illegal or "nefarious," the Ninth Circuit has explained that "it is settled that wire fraud does not require proof that the defendant's conduct violated a separate law or regulation, be it federal or state law." This is because the three elements of wire fraud include no requirement that the conduct be illegal. *United States v. Green*, 592 F.3d 1057, 1064 (9th Cir. 2010). As the elements likewise do not include a requirement that the conduct be nefarious, this logic extends to that portion of the argument as well. This argument therefore fails.

Defendant's argument that her conduct as alleged in the indictment does not constitute a material misrepresentation presents a novel question in a highly technical context. A district court in the Northern District of Illinois recently considered the question of misrepresentation in a comparably novel setting. *United States v. Vorely*, 420 F. Supp. 3d 784 (N.D. Ill. 2019). There, defendants allegedly placed "spoofed" commodities orders that they intended to withdraw before the orders could be filled, thus misleading traders about the true state of the market. *Id.* at 787. Defendants argued that the indictment charging them was insufficient as their conduct did not constitute a misrepresentation because there was no evidence that their orders constituted anything more than "good-faith bids." *Id.* at 789-805. The court disagreed and upheld the indictment, concluding that the "the wire fraud statute has long encompassed implied misrepresentations," and the question of whether the orders constituted good-faith bids was a question of fact to be resolved at trial. *Id.* at 806.

Here, as in *Vorely*, defendant's challenge to the indictment presents a question of fact that must be resolved at trial. At this stage, the government is not required to prove its case – it must merely allege facts that, if proved, would meet the elements of wire fraud. *Buckley*, 689 F.2d at 897. The indictment alleges that defendant misrepresented herself by concealing her identity and using stolen credentials, which made her appear to be a user with the requisite authority to send commands and access data within the accounts. This is sufficient because courts have found that "implicit false misrepresentations" demonstrate evidence of a scheme to defraud. *See United States v. Young*, 952 F.2d 1252, 1255–57 (10th Cir. 1991) (inferring intent to defraud a financial institution from defendant's misrepresentation that she was authorized to cash certain checks); *United States v. Briggs*, 965 F.2d 10, 12 (5th Cir. 1992) (concluding that "an implicit misrepresentation by [the defendant] that she was acting under her employer's authority [when she made unauthorized wire transfers from her employer's bank account] would be sufficient to establish . . . misrepresentation . . . ."); *United States v. Morgenstern*, 933 F.2d 1108, 1113 (2d Cir. 1991) (affirming a conviction under § 1344(2) where defendant implicitly misrepresented his authority to deposit checks). Thus, the indictment sufficiently alleges misrepresentation of a material fact – namely, defendant's identity and authority to access the relevant accounts. Any arguments that defendant's actions were innocuous should be resolved by the trier of fact.

2. *Element Three: Specific Intent*

Defendant argues that Count 1 of the indictment also fails because it does not allege that defendant had the specific intent to deceive and cheat victims out of property, nor that what defendant allegedly took from the victims qualifies as "property" under the wire fraud statute. Thus, the third element of wire fraud is not sufficiently alleged. Dkt. # 158 at 3-5.

Looking to the specific intent element of wire fraud, the Ninth Circuit has explained that "to be guilty of wire fraud, a defendant must act with the intent not only to make false statements or utilize other forms of deception, but also to deprive a victim of money or property by means of those deceptions." *United States v. Miller*, 953 F.3d 1095, 1101 (9th Cir. 2020), *cert. denied*, 141 S. Ct. 1085 (2021). In other words, intent to both "deceive and cheat" must be shown. *Id.* However, "it is not necessary to show that the scheme was successful or that the

intended victim suffered a loss or that the defendants secured a gain." *Schreiber Distrib. Co. v. Serv-Well Furniture Co.*, 806 F.2d 1393, 1400 (9th Cir. 1986); *see also United States v. Louderman*, 576 F.2d 1383, 1387 (9th Cir. 1978).

First, the Court addresses defendant's argument that the allegedly stolen data does not qualify as "property" under the wire fraud statute. Then, the Court turns to defendant's argument that the indictment does not adequately allege specific intent.

i. Property Under the Wire Fraud Statute

As a threshold manner, the parties debate whether the indictment sufficiently alleges that the data copied by defendant qualifies as "property" under the wire fraud statute. Defendant argues that for information to be "property" under the statute, it must qualify as property under state law. Dkt. # 158 at 4-5. Therefore, she argues, because the indictment does not sufficiently allege that the data taken from Capital One would be a trade secret under Washington law, it cannot be considered property in the wire fraud context. *Id.* The government argues that the data defendant downloaded qualifies as property because it is "confidential business information." Dkt. # 131 at 8 n.4.

In *Carpenter*, the Supreme Court recognized that "[c]onfidential business information has long been recognized as property," and accordingly meets the "property" requirement in the mail and wire fraud statutes. *Carpenter v. United States*, 484 U.S. 19, 25-26 (1987). However, defendant correctly indicates that this seemingly clear statement has recently been reexamined by other district courts in our circuit. In *Planned Parenthood*, the court found that the question of whether information is property for purposes of wire fraud, "must be determined by reference to applicable state laws." *Planned Parenthood Fed'n of Am., Inc. v. Ctr. for Med. Progress*, 214 F. Supp. 3d 808, 822 (N.D. Cal. 2016), *aff'd on other grounds by*, 890 F.3d 828 (9th Cir.), *amended by*, 897 F.3d 1224 (9th Cir. 2018), *and* 735 F. App'x 241 (9th Cir. 2018). The court agreed with defendants that "confidential information can only constitute 'property' under the state laws at issue if the information meets the definition of a trade secret under the Uniform Trade Secrets Act, as adopted by those states." *Id.* at 822-23; *see also United States v. Abouammo*, No. CR19-621EMC, 2021 WL 718842 (N.D. Cal. Feb. 24, 2021).

Although state law is a valid source for defining the scope of property rights protected by federal laws, it is not the sole source. *See Ruckelshaus*, 467 U.S. at 1001 (noting that "property interests . . . are created and their dimensions defined by existing rules or understandings that stem from an independent source *such as* state law" (emphasis added)). Furthermore, both the Ninth Circuit and the Supreme Court have cited the *Carpenter* decision to acknowledge a property right in confidential business information under the wire fraud statue – without any reference to state property law. *See Cleveland*, 531 U.S. 12, 19 (2000) ("Citing decisions of this Court as well as a corporate law treatise, we observed [in *Carpenter*] that "[c]onfidential business information has long been recognized as property."); *United States v. Yates*, 16 F.4th 256, 265 (9th Cir. 2021) (recognizing a "property right in trade secrets *or confidential business information*" under the wire fraud statute (emphasis added)). Other circuit courts have similarly accepted confidential business information as property under *Carpenter* without reference to underlying state law. *See, e.g.*, *United States v. Poirier*, 321 F.3d 1024, 1030 (11th Cir. 2003); *United States v. Hager*, 879 F.3d 550, 555 (5th Cir. 2018) ("We also reject [defendant's] argument in the alternative that, even if intangible property interests are protected under §§ 1341 and 1343, those interests are limited solely to trade secrets as defined by state law."); *United States v. Mahaffy*, 693 F.3d 113, 135 (2d Cir. 2012) ("Information may qualify as confidential under *Carpenter* even if it does not constitute a trade secret.").

Accordingly, a straightforward application of *Carpenter* in this case compels the conclusion that if the data allegedly copied from Capital One is "confidential business information," it is property under the wire fraud statute. This data includes "personal identifying information from approximately 100,000,000 customers who had applied for credit cards from Capital One." Dkt. # 166 at ¶ 19. In *Louderman*, the Ninth Circuit found that "confidential internal information concerning telephone customers or post office box holders" was property under the wire fraud statute where "the object of the scheme to defraud here was . . . to obtain intangible, commercial information which the telephone company and post office chose to keep confidential and which its customers expected would remain confidential." *United States v. Louderman*, 576 F.2d 1383, 1386-87 (9th Cir. 1978). Because the Capital One data described in the indictment

similarly contains information concerning credit card applicants that was meant to remain confidential, it is sufficiently alleged to be confidential information. The government has therefore adequately alleged that the copied data is "property" under the wire fraud statute.

ii. Intent to Deceive and Cheat

Accepting that the government has sufficiently alleged the Capital One data qualifies as property under the wire fraud statute, the Court now turns to defendant's argument that the indictment fails to allege she had the requisite specific intent to defraud. The Ninth Circuit has held that this means that defendant must have acted "with the intent not only to make false statements or utilize other forms of deception, but also to deprive a victim of money or property by means of those deceptions." *Miller*, 953 F.3d at 1101.

Here, defendant argues that that the indictment "does not allege anywhere how she deceived and cheated any of the victims of money or property." Dkt # 122 at 6. In particular, she argues that the indictment does not allege that she possessed the requisite specific intent because it "fail[s] to establish that she would have known the content of what was downloaded beforehand and there is no evidence she monetized that data (or any other data) once it was copied." Dkt. # 158 at 2; *see also* Dkt. # 122 at 6.

The question of whether defendant monetized the data is inconsequential. The law requires that she acted with intent to deprive the victim of "money *or property*." *Miller*, 953 F.3d at 1101 (emphasis added). As discussed above, the data constitutes property. The law does not ask what she intended to do with it next. *Cf. Carpenter*, 484 U.S. at 26-27 ("[Defendant] cannot successfully contend . . . that a scheme to defraud requires a monetary loss . . . it is sufficient that the [victim] has been deprived of its right to . . . exclusivity . . . ."); *Schreiber Distrib. Co.*, 806 F.2d at 1400 (stating that there is no need for the government to show that the "scheme was successful or that . . . the defendants secured a gain"). Thus, that defendant is not alleged to have monetized the data is irrelevant to the validity of the indictment.[4]

[4] Although it could, of course, have a significant impact at sentencing.

As to defendant's argument that she did not know what she was downloading, this is a question of fact that can be raised at trial. *See Kelly*, 874 F.3d at 1046.

Defendant's general argument that the indictment does not "allege anywhere how she deceived and cheated any of the victims of money or property" is incorrect. Dkt. # 122 at 6. Intent to defraud may be demonstrated through circumstantial evidence. *United States v. Lothian*, 976 F.2d 1257, 1267-68 (9th Cir. 1992) ("It is often difficult to prove fraudulent intent by direct evidence and it must be inferred in such cases from a pattern of conduct or a series of acts, aptly designated as badges of fraud."). The indictment includes numerous allegations of circumstantial evidence of intent.

As the government argues, defendant's intent to deceive and cheat can be inferred circumstantially by her alleged "pattern of conduct, including (1) creating and using scanners that allowed her to identify servers with misconfigured web application firewalls; (2) 'transmitti[ing] commands to the misconfigured servers that obtained the security credentials for particular accounts or roles belonging' to the victims; (3) using the security credentials 'to obtain lists or directories of folders' of data on the victims' cloud storage space; (4) using the stolen credentials 'to copy data, from folders or buckets of data' in the victims' cloud storage space; (5) implicitly representing that the commands she sent to the servers were legitimate and came from a user with permission to send such commands; (6) using VPNs and TOR to conceal her location and identity while taking these actions; and (7) using 'her unauthorized access to certain victim servers—and stolen computing power of those servers—to "mine" cryptocurrency for her own benefit.'" Dkt. # 131 at 8-9; Dkt # 166 at ¶¶ 12-21. These actions, if proved, provide circumstantial evidence that defendant intentionally used "deception" to deprive victims "of money or property." *Miller*, 953 F.3d at 1101.

To the extent that defendant argues that the indictment fails to allege intent because the alleged circumstantial evidence could also support innocuous behavior, whether or not there is also an "innocent explanation for defendant's conduct" is a question of evidence to be determined at trial. *Green*, 592 F.3d at 1066. The Court must only determine whether the government has sufficiently alleged facts that, *if proven*, support a finding of specific intent to

deceive the named victims and deprive those victims of property. *See Buckley*, 689 F.3d at 900 ("[T]he weakness of the Government's case is irrelevant to the sufficiency of the indictment."). Here, the indictment contains sufficient alleged facts to support a finding of specific intent.

B. Specificity

Defendant also argues that Count 1 of the superseding indictment should be dismissed because it "lacks the requisite specificity." Dkt. # 122 at 1. In an indictment, "the Government need not allege . . . its case theory or the evidence underlying the charges. The Government must only provide enough facts to apprise a defendant of what defense should be prepared for trial." *United States v. Holmes*, No. CR18-258EJD, 2020 WL 666563, at *6 (N.D. Cal. Feb. 11, 2020); *see also Buckley*, 689 F.2d at 900 (explaining that the indictment stage "is not the appropriate time to require the Government to present its proof"). For example, in *Russell*, the Supreme Court found an indictment invalid where defendants were convicted of refusing to answer certain questions posed by a congressional subcommittee, but the indictment failed to identify the subject matter of the inquiry (a necessary component of the underlying charge). *Russell v. United States*, 369 U.S. 749 (1962). Similarly, in *Cecil*, the Ninth Circuit held a "rather barren" indictment, which essentially tracked the text of the relevant conspiracy statutes and only made "two specific allegations" (identifying the locations of the conspiracy and the names of the alleged conspirators), was invalid due to its "glaring lack of factual particularity." *United States v. Cecil*, 608 F.3d 1294, 1294-97 (9th Cir. 1979).

Here, defendant argues that the scheme (1) "fails to provide sufficient detail to apprise Ms. Thompson of what misrepresentations or concealments of material fact she has made—and as to which victims," Dkt. # 122 at 7; (2) "fails to describe how Ms. Thompson purportedly intended to cause any amount of loss to any of the alleged victims," *Id.* at 1; (3) "does not allege with specificity the data allegedly stolen from the other entities," *Id.* at 3; and (4) "does not specify which of the entities' rented server Ms. Thompson allegedly utilized to mine cryptocurrency nor how the alleged mining of cryptocurrency harmed any of the victims' rented servers or otherwise 'cheated' the victims," *Id.*

As to the misrepresentations made by defendant, the indictment alleges, for example, that defendant used stolen security credentials to misrepresent herself as an authorized user of the victim accounts. Dkt. # 166 at ¶ 16; *see supra* Section I.A.1. As to which victims these misrepresentations were made to, the indictment alleges, for example, that defendant used stolen credentials to wrongfully download data from all eight of the victims enumerated in the indictment. *Id.* at 5. As to her intent to cause loss to the victims, the indictment has sufficiently alleged facts that, if proven, provide circumstantial evidence of specific intent to, at the least, deprive the victims of their right to exclusivity in their property. *Id.* at 3-5; *see supra* Section I.A.2.ii. As to defendants' final arguments, she is right to note that the indictment does not specify what data was allegedly stolen from the victims other than Capital One, nor does it identify which servers were allegedly used for crypto mining. However, because the indictment identifies which victims allegedly had data stolen, and implicitly limits the crypto mining victims to the pool of eight identified victims,[5] the indictment is "clear enough to give the defendant[] notice of the crime charged and to allow [her] to plead double jeopardy," and thus meets the baseline set forth by Rule 7. *Buckley*, 689 F.2d at 898. Whether the government is required to provide more detailed information is a question to be analyzed with reference to defendant's request for a bill of particulars.

Finally, defendant argues that the indictment does not allege how defendant's alleged crypto mining harmed the victims. However, showing harm to the victim is not a required element of wire fraud. *Schreiber*, 806 F.2d at 1400.

Because the indictment sufficiently alleges wire fraud, defendant's motion to dismiss Count 1 of the indictment is denied. Because defendant's arguments for dismissing Counts 9 and 10 were predicated on the dismissal of Count 1, defendant's motion to dismiss Counts 9 and 10 is also denied.

[5] The indictment specifies that defendant used "certain victim servers" for her crypto mining operation. Dkt. # 166 at ¶ 21.

II. Bill of Particulars

Defendant argues that even if Count 1 of the indictment is upheld, the court should order the government to provide a bill of particulars. Federal Rule of Criminal Procedure 7(f) empowers the Court to direct the government to file a bill of particulars. The decision to order a bill of particulars is within the Court's broad discretion. *Will v. United States*, 389 U.S. 90, 98-99 (1967).

While neither a bill of particulars nor "open file" discovery can cure an otherwise invalid indictment, *Cecil*, 608 F.2d at 1296; *Russell*, 369 U.S. at 770, a bill of particulars is the proper remedy where an indictment satisfies Rule 7(c) but nonetheless contains ambiguities that would prevent a defendant from being adequately prepared for trial. *See United States v. Long*, 706 F.2d 1044, 1054 (9th Cir. 1983) (citing *Will*, 389 U.S. at 99; *United States v. Clay*, 476 F.2d 1211, 1215 (9th Cir. 1973)). A bill of particulars is therefore "designed to apprise the defendant of the specific charges being presented to minimize danger of surprise at trial, to aid in preparation and to protect against double jeopardy." *Id.* (citing *United States v. Davis*, 582 F.2d 947, 951 (5th Cir. 1978), *cert. denied sub nom.*, *Clayton v. United States*, 441 U.S. 962, *rehr. denied*, 442 U.S. 948 (1979)). The purpose of a bill of particulars is not to allow the defendant to obtain full discovery of the government's evidence. *United States v. Giese*, 597 F.2d 1170, 1181 (9th Cir. 1979), *cert. denied*, 444 U.S. 979 (1979). However, in some cases, "full discovery obviates the need for a bill of particulars." *Id.* at 1180-81; *see also United States v. Clay*, 476 F.2d 1211, 1215 (9th Cir. 1973) (finding no abuse of discretion where the trial court denied the motion for the bill but granted full discovery).

Defendant argues that Count 1 of the indictment fails to provide sufficient detail to allow her to adequately prepare for trial. Dkt. # 122 at 7. In defendant's view, the government's bill of particulars should "identify with specificity and as to every separate victim entity listed in Count 1 the following: (a) the particular misrepresentations or concealments of material fact; (b) who or what made the particular misrepresentations or concealments of material fact; (c) to whom the particular misrepresentations or concealments of material fact were made; (d) the date the misrepresentations or concealments of material fact were made;" "(e) the manner in which the

representations were false, fraudulent, or fraudulently misleading," *id.* at 8, and (f) "provide specific facts sufficient to evidence Ms. Thompson's intent to both deceive and cheat the victims specified in Count 1, that is, facts sufficient to demonstrate that she intended to cause loss to each and every separate victim alleged in Count 1."[6] *Id.* at 9.

The government responds the indictment itself provides details of the alleged offense, rendering a bill of particulars unnecessary. Dkt. # 131 at 10 (citing *Giese*, 597 F.2d at 1180). Further, the government argues that even if defendant required additional information to prepare a defense, the "Court should consider 'all other disclosures made by the government.'" *Id.* (quoting *Long*, 706 F.2d at 1054). Here, the government notes, defendant has been provided with "considerable additional information," including (1) "a meeting during which the government detailed its investigation;" (2) "production of searchable, indexed, electronic discovery;"' and (3) "disclosure of grand jury transcripts and exhibits." *Id.*

Given the detail in the indictment, the Court finds many of defendant's requests for the bill of particulars unnecessary. As to requests (a), (b) and (e), regarding particular misrepresentations and who made them, the indictment alleges that by using "stolen security credentials," and otherwise obscuring her identity, defendant misrepresented herself as an authorized user. Dkt. # 166 at ¶¶ 16-18.

As to request (c) regarding to whom the misrepresentations were made, the indictment alleges that defendant used the stolen security credentials to copy and download data from all eight victims listed in the Background section of the indictment. Dkt. # 166 at ¶¶ 13-15, 19-20.

[6] To the extent that defendant argues that the government must establish that defendant knew each victim she was defrauding, the Ninth Circuit has made clear that this is not a requirement for a wire fraud conviction. In *Crawford*, the defendant argued that there was insufficient evidence to uphold her wire fraud conviction where she had sold a painting that did not belong to her, but where the actual owner of the painting had not yet been established. *United States v. Crawford*, 239 F.3d 1086, 1092. The Ninth Circuit upheld the conviction, finding that specific intent was met with proof that defendant knew she did not own the painting, and she intended to deprive the owner, whoever that might be, of its use. *Id.* at 1093.

As to request (d), regarding the date the misrepresentations were made, the indictment alleges that defendant copied Capital One's data on or about March 22, 2019.[7] Dkt. # 166 at ¶ 23. Furthermore, the indictment specifies that the alleged activities took place "[b]eginning or before March 2019 and continuing until on or about July 17, 2019." *Id.* at ¶ 1. Regarding the specific dates relating to other victims, defendant is not entitled to this level of detail in the indictment. The Ninth Circuit has explained that "request[s] for the 'when, where, and how' of every act" in a scheme is "equivalent to a request for complete discovery of the government's evidence, which is not a purpose of the bill of particulars." *Giese*, 597 U.S. at 1181; *see also Holmes*, 2020 WL 666563, at *8-9 (declining to require government to include specific dates that false representations were made in bill of particulars); *United States v. Feil*, No. CR09-863JSW, 2010 WL 1525263, at *3 (N.D. Cal. Apr. 15, 2010) (finding bill of particulars is not warranted to obtain "precise timing").

Finally, as to request (f), specific intent under the wire fraud statute can be proven with circumstantial evidence, which has been adequately alleged in the indictment. *See supra* section I.A.2.ii.

However, the indictment does not allege with specificity the nature of the data allegedly downloaded from victims other than Capital One, nor which victims' servers were allegedly used for defendant's crypto mining operation. Given that wire fraud requires that "the thing obtained must be property in the hands of the victim," *Cleveland*, 531 U.S. at 15, defendant's ability to argue that the data is not "property," and thus that she lacked specific intent, is significantly hampered by not knowing what data she allegedly downloaded. Additionally, the generic reference to "certain victims' servers" used for crypto mining also warrants clarification to minimize the danger of surprise at trial. Therefore, the Court orders that the government provide defendant with a bill of particulars specifying the data downloaded from victims other

[7] The indictment also lists five more dates on which defendant used stolen security credentials to access the servers of other victim entities to obtain information in relation to other charges, Dkt. # 166 at ¶¶ 27, 29, and the government provided defendant a PowerPoint detailing its investigation.

than Capital One, as well as which victims' servers were used in defendant's crypto mining operation.

For all of the foregoing reasons, IT IS HEREBY ORDERED that:

1. Defendant's motion to dismiss Counts 1, 9, and 10 of the indictment (Dkt. # 122) is DENIED.
2. Defendant's motion for a bill of particulars (Dkt. # 122) is GRANTED in part and DENIED in part. The government is ordered to provide the bill of particulars specified in this Order by March 11, 2022.

DATED this 28th day of February, 2022.

Robert S. Lasnik
United States District Judge